TALLINN UNIVERSITY OF TECHNOLOGY
Faculty of Information Technology
Department of Computer Science
Chair of Network Software

Sinowal Trojan

ITX8032 Infosüsteemide Ründed ja Kaitse: homework

Student: Konstantin Saveljev
Student code: 030548IAPM
Supervisor: Toomas Lepik

Tallinn
2008

Table of Contents

List of Figures

Introduction

Before 2005 there were no known rootkits for Windows (any 32 bit version of that operation system) which infected the master boot record (MBR). Researchers had an idea that it was theoretically possible but there were no solutions seen yet. But in 2005, researchers Derek Soeder and Ryan Permeh of eEye Digital Security showed the idea was possible by producing proof-of-concept code, called “BootRoot” [1].

February 2006. First reports are gathered on Sinowal (also known as Mebroot or Torpig) trojan which uses the same approach as in harmless BootRoot but has its own modifications which makes this trojan dangerous for a common user.

November 2008. New wave of news about Sinowal shocks the world (of course there were news about this trojan and its modifications throughout 2006-2008 period but now they have made a huge discovery on the stolen data). According to the RSA FraudAction Research Laboratory, this trojan has stolen and compromised login credentials from about 500,000 online bank accounts and credit and debit cards over the course of nearly three years [2].

1 Task

The main goal of this paper is to give a detailed analysis of how Sinowal trojan behaves, difficulties in defending against it and overview of impact on an average user.

We will begin with an overview of Sinowal's parts: bootkit and backdoor. Some parts of how things work (installation, user data theft) will be discussed in more details. We will then try to identify the difficulties with which antivirus companies deal when trying to protect their users from this trojan. Finally we will have a look at the impact of this crimeware on normal unaware users.

2 Detailed analysis of Sinowal trojan.

Sinowal trojan can be represented as two huge and complex (and advanced) parts. The first part is the bootkit which makes this trojan almost invisible on your system. The other part is the backdoor which attempts to steal as much user data as possible (most effort done on collecting user data to a range of online banking systems).

Before Sinowal can start operating it has to get on your machine. Thousands of malicious web pages have been created just for this purpose. When user visits any of those pages a special generated code is being run which tries to exploit vulnerability in the browser which is used by the unaware user. If the exploitation succeeds a malicious program is being downloaded to the user's machine. Sophos (antivirus and anti-spam company) has claimed to be finding over 6,000 newly infected pages daily – that's one every 14 second [3].

2.1 Bootkit

Once on the victim machine, the malicious code modifies the MBR, writes the rootkit part to a disk, sector, extracts a Windows backdoor from itself, install the backdoor, and then deletes itself [4]. More detailed behavior is represented on Figure 1.

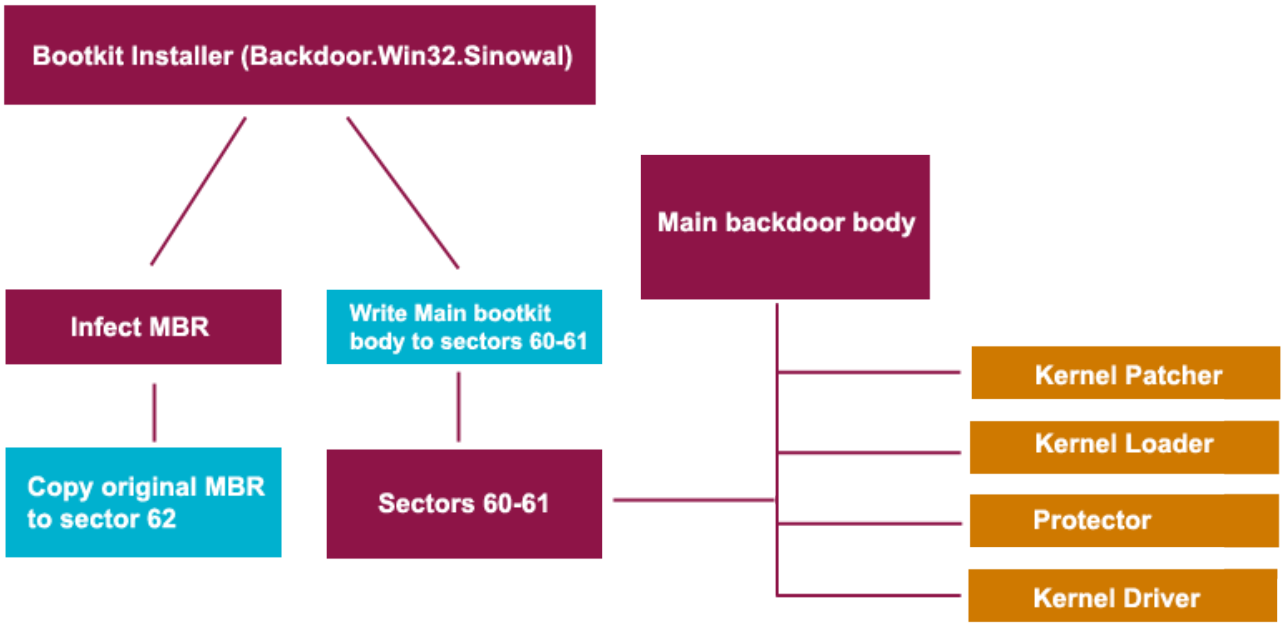

Figure 1: Sinowal trojan installer behavior

The hardest part for trojan here is to gain access to MBR. According to Microsoft [5] Sinowal is trying to modify MBR using the CreateFile API attempting to open "\Device\Harddisk0\DR0" for write access. Using the CreateFile API in this way (for direct/raw disk access) requires administrative privileges. So if the user is logged into Windows as a standard user or if he/she is using Windows Vista with UAC enabled, even if the malware installer is run accidentally or via some exploit code, it will be running with insufficient privilege to modify the hard disk MBR; thus it will not be able to persist a system restart.

But when this trojan succeeds in infecting the MBR, instructions pass control to the main part of the rootkit which is placed on several hard disk sectors and which is not represented as files in the system. This part monitors the already loaded Windows operating system and when reading, it hides the infected MBR and the "dirty" sectors by presenting clean ones instead. It does this by intercepting and substituting system functions (Figure 2) [4].

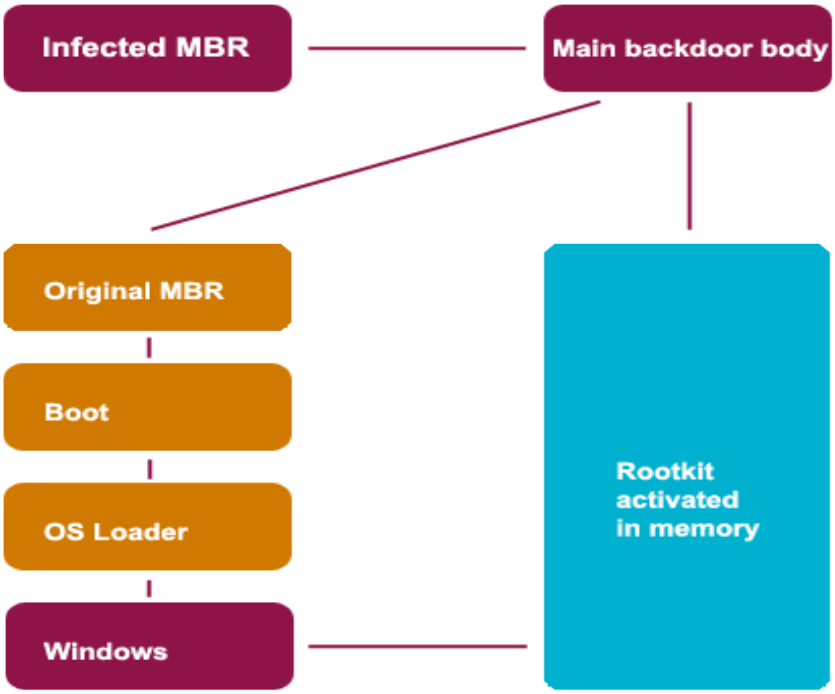

Figure 2: Infected (with Sinowal) system startup

2.2 Backdoor

In addition to hiding its presence in the system, the malicious code installs a backdoor in Windows. Upon execution, it drops some files into the system (might differ for different versions) [7]:

- `%programfiles%\common files\microsoft shared\web folders \ibm<5-digit randrom number>.dll - Trojan-PSW.Win32.Sinowal.co`
- `%programfiles%\common files\microsoft shared\web folders \ibm<5-digit randrom number>.dll - Trojan-PSW.Win32.Sinowal.co`
- `%windir%\temp\$_2341233.tmp`
- `%windir%\temp\$_2341234.tmp`
- `%windir%\temp\$_2341235.tmp`
- `%windir%\temp\$b17a2e8.tmp`

It installs itself as a service and adds this Registry key launch point [7]:

- Key:HKLM\System\ControlSet001\Services\gb
  File: %programfiles%\common files\microsoft shared\web folders
  \ibm<5-digit random number>.dll

This trojan attempts to steal different system and account information from the infected machine. Stolen information may be the following [7]:

- IMAP/POP3/SMTP username, passwords, server information from mail clients such as AK-Mail, Thunderbird, TheBat
- Bookmarks
- E-mail addresses from the Windows Address Book
- Passwords and other data stored from FTP clients such as Trellian FTP, WS_FTP, Total Commander, Crystal FTP Pro and GlobalSCAPE

It also monitors web browser such as Internet Explorer, Firefox, Opera for online banking information upon access on the banking sites. During its evolution the list of those sites has grown to around 2,500.

Next come a research results done by David Bizeul who had a case study on Torpig/Sinowal during July 21st 2007 – October 10th 2007 [6]. We may assume that these results don't differ from what you can find when exploring new modifications of Sinowal, the only huge difference will be the amount of data this trojan is trying to steal.

First, David Bizeul checked some of the IP addresses the trojan was using to communicate with and connected on http://194.146.207.18/config (doesn't work on the day of the paper writing) where he got a page with a very interesting content:

```
storage_send_interval=”600”
config_file =”$_2341234.TMP”
starage_file =”$_2341233.TMP”
www_domains_list = “pageshowlink.com”
redirector_url =”citibusinessonline.da-us.citibank.com /cbusol/uSignOn.do {www}
/usa/citibusiness.php 2 0 3”
redirector_url = "*fineco.it /fineco/PortaleLogin {www} /it/fineco.php 2 0 3"
```

```
redirector_url = "onlineid.bankofamerica.com /cgi-bin/sso.login.controller* {www}
/usa/boa_pers/sso.login.php 2 0 2"
redirector_url = "onlinebanking-nw.bankofamerica.com /login.jsp* {www}
/usa/boa_pers/sso.login.php 2 0 2"
redirector_url = "online.wellsfargo.com /signon* {www} /usa/wellsfargo.php 2 0 2"
… (more config lines here)
```

That file turned out to be a configuration file for our banking trojan. All indicated urls were targets which the trojan had to redirect on malicious site.

Let's explore one of those lines:

```
redirector_url = "*fineco.it /fineco/PortaleLogin {www} /it/fineco.php 2 0 3"
                   _______    ___________________   ___   ____________  _____
                     1            2                 3        4          5
```

The portions of that line represent different fields:

1. domain name
2. end of the ligitimate url
3. protocol used (http)
4. target redirected location (end of the URL)
5. ?

It's clear that's one data is missing: the target domain. This domain was probably obtained through www_domains_list pointing on *pageshowlink.com* (parking page during the investigation).

As you can see Sinowal is highly configurable and allows to make a huge list of different content we want to intercept. Next chapter will try to explain why it is very difficult for antivirus companies to fight this trojan.

3 Defense against Sinowal trojan

Since Sinowal loads before anything else, it is nearly invisible to security software. “You can't execute any earlier than that,” said Mikko Hypponen, F-Secure's chief research officer [1].

The main problem for antivirus companies to fight Sinowal is because of its bootkit feature [4]:

1. The malicious code gains control before the operating system starts, and, consequently, before the antivirus program starts
2. It's difficult to detect the interception of functions from within an infected operating system
3. Restoring intercepted functions can lead to the entire operating system crashing
4. Curing the MBR is only possible if the original MBR can be detected.

Of course, the best protection is not to let any malicious program on your computer. Some antivirus programs can detect harmful programs even when those are 0day trojans or viruses etc. Though there is always a possibility that such protection can be penetrated, and this raises the question of how to disinfect an already infected machine.

The first option we have is a machine with antivirus software preinstalled. Then it really depends on the quality of that software and how it can handle those 4 points described above.

The second option is when our machine has no antivirus software installed and we need to install it first. Here we encounter an additional problem related to that one described in point 1;

the malicious code can block attempts to install an antivirus solution on the infected system.

Sinowal writes also don't sleep and improve their crimeware. What they do is they analyse how antivirus software solve the problems listed above and change/update their code to make those solutions not work at all. Figure 3 shows another problem for antivirus software companies. The amount of different modifications of Sinowal is very big and the new version keep showing up.

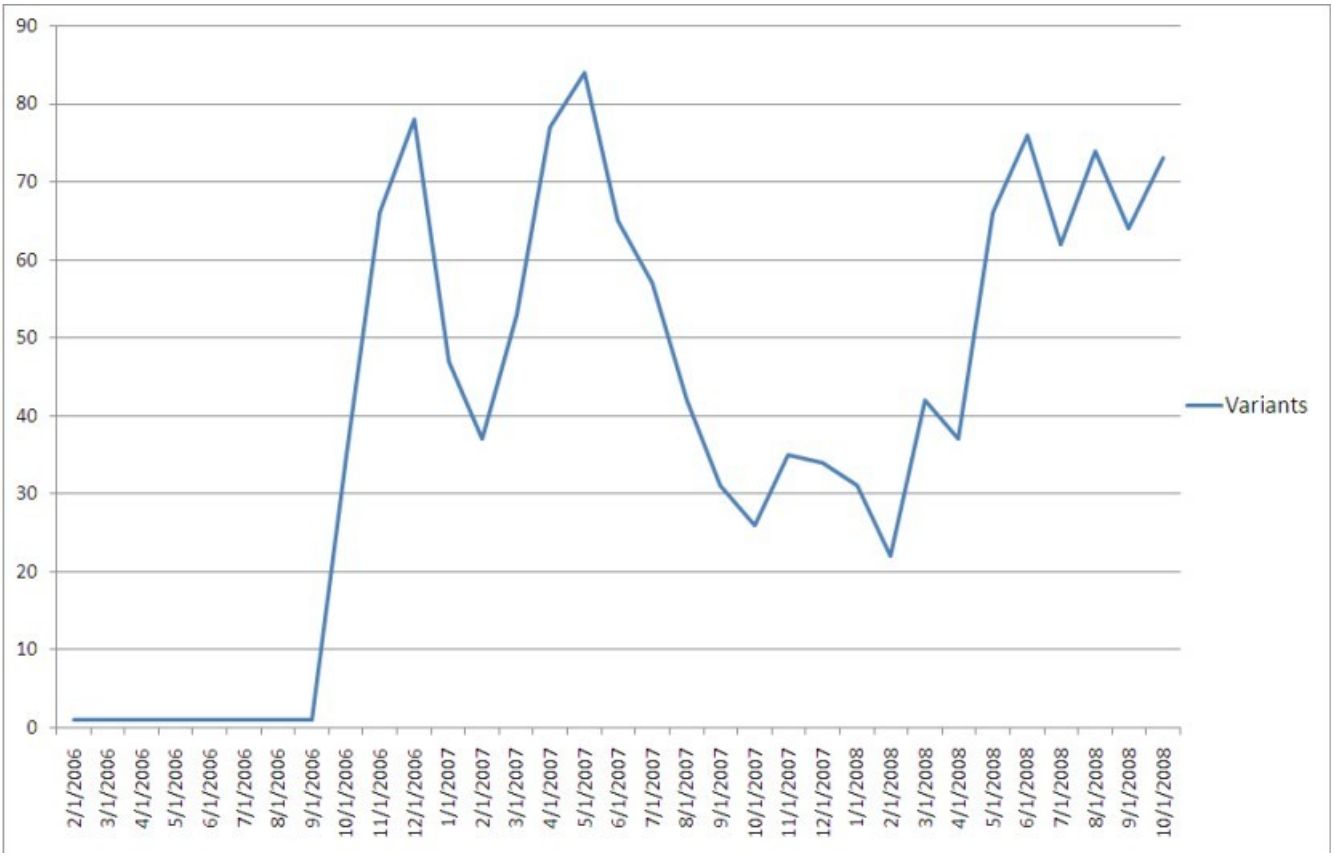

Figure 3: Sinowal modifications since its first version

4 User impact

There are so many unexperienced users out there that any virus/trojan etc. will have its own targets found. But when it comes to Sinowal we talk about a professional product. It has a purpose and writers are motivated by the amount of “free money” out there in the Internet.

Every major version/modification of Sinowal comes with new workarounds to fool the antivirus software and the users. During these new major versions no one is secured from it. All we can do is to trust our antivirus software companies that they will deal with it as fast as they can and add it to their database as soon as possible. Figure 4 shows how those major versions of Sinowal progress since the first launch of the crimeware.

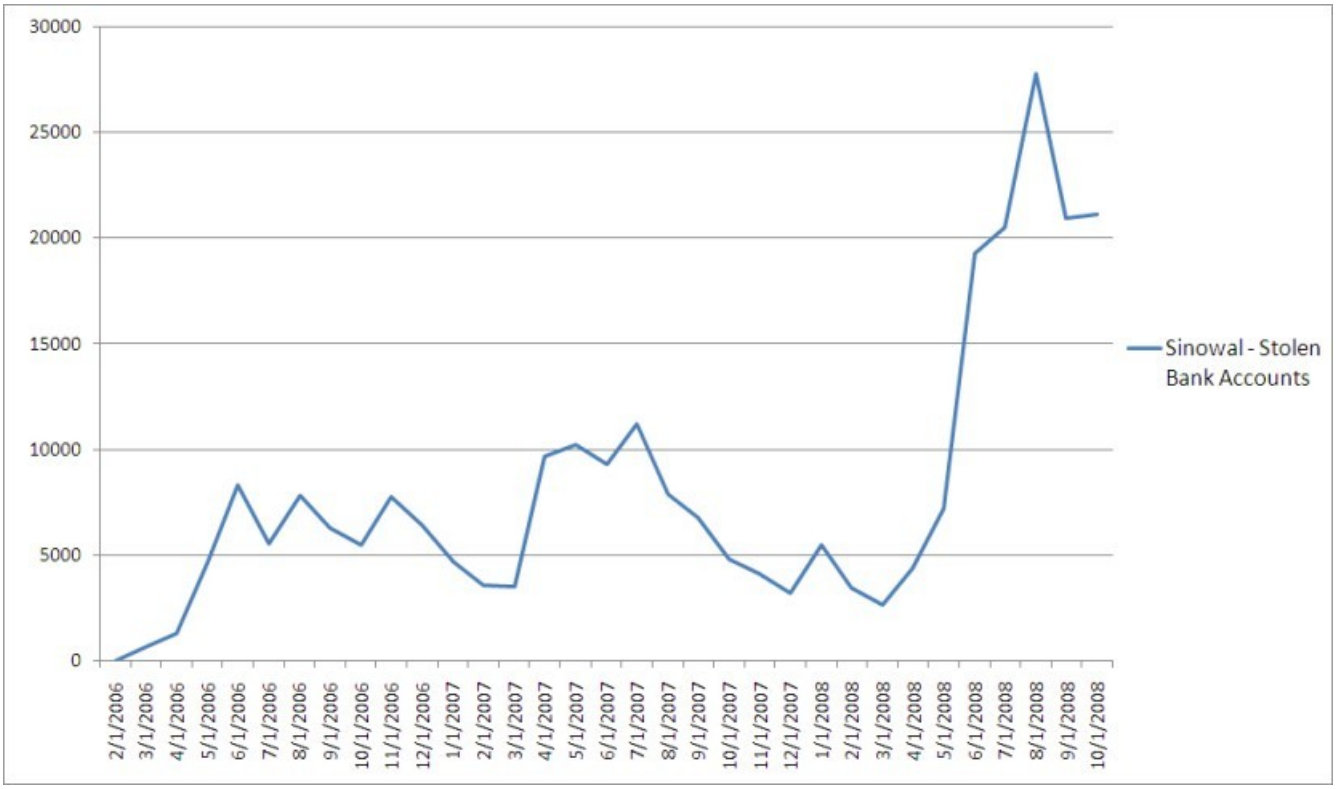

Figure 4: Number of stolen bank accounts since first version of Sinowal

Conclusion

Throughout this work it was shown how complex and professionally organized Sinowal trojan is. The main two parts of the trojan – bootkit and backdoor – make this trojan one of a kind at the moment. Antivirus companies have difficulties with this trojan because of the enormous new variants appearing in the Internet. Lots of personal account information has been stolen during these 3 years, how much more will be stolen till we find an optimal solution to fight this type of crimeware?

The aim of this work was to introduce you to the technology used in Sinowal trojan and give you a detailed analysis of how it works. I think the aim has been reached.

Bibliography

1. Mebroot proves to be a tough rootkit to crack. [WWW] http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9066585
2. RSA Unravels Sinowal Trojan. [WWW] http://www.enterpriseitplanet.com/security/news/article.php/3783641
3. Sinowal Trojan Stealing Banking Information. [WWW] http://news.digitaltrends.com/news-article/18302/sinowal-trojan-stealing-banking-information
4. Viruslist.com – Malware evolution: January – March 2008. [WWW] http://www.viruslist.com/en/analysis?pubid=204792002
5. Anti-Malware Engineering Team : MBR rootkit: VirTool:WinNT/Sinowal.A report. [WWW] http://blogs.technet.com/antimalware/archive/2008/01/10/mbr-rootkit-virtool-winnt-sinowal-a-report.aspx
6. Russian Business Network Study. / David Bizeul [WWW] http://www.bizeul.org/files/RBN_study.pdf
7. F-Secure Malware Information Pages: Trojan-PSW:W32/Sinowal.CP. [WWW] http://www.f-secure.com/v-descs/trojan-psw_w32_sinowal_cp.shtml